WPI

TI - Authorized person judging system - compares one thyme password with user password from client, for confirmation of authorized person

AB - JP11306141 NOVELTY - When a host computer (50) receives a decision demand, it generates a random number and sends it to the client. One thyme password is generated by one thyme password generator which is compared with user password, from client in the host computer for confirmation.
- USE - For authentication of person using client computer.
- ADVANTAGE - Leakage of information to people with identical voice is avoided, thereby secrecy is retained reliably. DESCRIPTION OF DRAWING(S) -- The figure shows the functional block diagram of authorized person judging apparatus. (50) Host computer.
- (Dwg.1/5)

PN - JP11306141 A 19991105 DW200004 G06F15/00 008pp

PR - JP19980113921 19980423

PA - (NIDE) NIPPON DENKI ENG KK

MC - T01-C08A T01-E04 T01-H01C2 T01-H07C5 T01-J12C W01-A05B W04-V

DC - P85 T01 W01 W04

IC - G06F15/00 ;G09C1/00 ;H04L9/32

AN - 2000-044577 [04]

PAJ

TI - QUALIFIED PERSON DECISION DEVICE

AB - PROBLEM TO BE SOLVED: To keep secrecy more securely through client's easy operation.
- SOLUTION: A random number generated by a random number generation part 43 on the side of a host computer 5 as a qualified person decision device at a decision request is reported to a client terminal 10 through a telephone line, the password of a client is ciphered by using the same random number and the same ciphering system by EX-OR parts 23 and 45 and data encoding parts 24 and 46 on both sides of a client computer 20 and the host computer 50 to generate a one-time password; while the one-time password is stored in a one-time password table 52, the one-time password is sent to a password reception part 54 through a data line different from the telephone line through which the random number was reported to gather them on the host computer 50, and a data matching part 55 confirms matching between the both to decide the qualified person.

PN - JP11306141 A 19991105

PD - 1999-11-05

ABD - 20000229

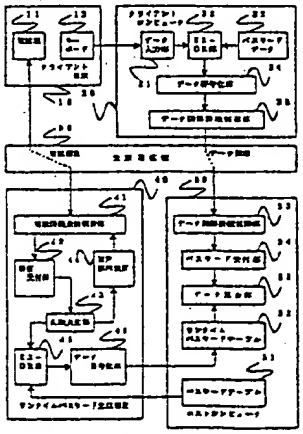
ABV - 200002

AP - JP19980113921 19980423

PA - NEC ENG LTD

IN - MOCHIZUKI KEIICHI

I - G06F15/00 ;G09C1/00 ;H04L9/32



<First Page Image>

(19)日本国特許庁（J.P）　(12)公開特許公報(A)　(11)特許出願公開番号
特開平11－306141
(43)公開日　平成11年(1999)11月5日

(51)Int.Cl.⁶	識別記号	FI	
G06F 15/00	330	G06F 15/00	330B
G09C 1/00	660	G09C 1/00	660E
H04L 9/32		H04L 9/00	673A
			673D

審査請求　未請求　請求項の数3　OL　（全8頁）

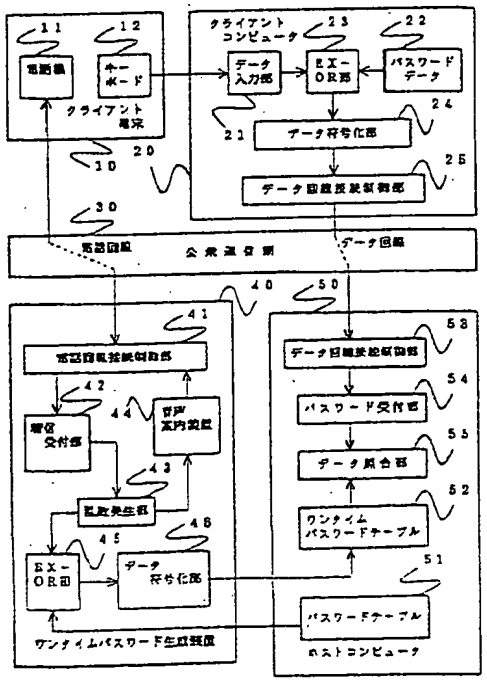
(21)出願番号　特願平10－113921

(22)出願日　平成10年(1998)4月23日

(71)出願人　000232047
日本電気エンジニアリング株式会社
東京都港区芝浦三丁目18番21号
(72)発明者　望月　慶一
東京都港区芝浦三丁目18番21号　日本電気エンジニアリング株式会社内
(74)代理人　弁理士　京本　直樹　（外2名）

(54)【発明の名称】　有資格者判定方式

(57)【要約】
【課題】　クライアントの簡単な操作で、更に秘密性の保持が確実にできる。
【解決手段】　判定要求の際に有資格者判定装置であるホストコンピュータ５０側の乱数発生部４３で発生する乱数をクライアント端末１０に電話回線を介して通知し、クライアントコンピュータ２０とホストコンピュータ５０との両方それぞれの側でＥＸ－ＯＲ部２３、４５およびデータ符号化部２５、４６により同一の乱数および同一の暗号化式を用いてクライアントのパスワードを暗号化してワンタイムパスワードを生成し、生成されたワンタイムパスワードを、一方ではワンタイムパスワードテーブル５２に格納し、他方では乱数を通知した電話回線とは別のデータ回線を用いてパスワード受付部５４に送ることによりホストコンピュータ５０に集め、データ照合部５５が双方の照合一致を確認して有資格者を判定している。



【特許請求の範囲】
【請求項1】　クライアントから入力されるパスワードにより有資格者を判定する有資格者判定方式において、有資格者の判定を行う有資格者判定装置側では、一つの通信回線を介して有資格者の判定要求を受けた際に乱数を発生して前記クライアントに通知すると共にこのクライアントに対して予め定められたパスワードに前記乱数を加味し所定の暗号化式により一回限りのワンタイムパスワードを生成するワンタイムパスワード生成装置と、クライアント側では、有資格者の判定要求をした際に受けた前記乱数を自己のパスワードに加味し前記暗号化式により一回限りのワンタイムパスワードを生成し前記通信回線とは別の通信回線を介して前記有資格者判定装置へ送るワンタイムパスワード再生装置とを備え、前記有資格者判定装置が、前記ワンタイムパスワード生成装置で生成したワンタイムパスワードと前記ワンタイムパスワード再生装置で生成したワンタイムパスワードとの一致を確認して有資格者と判定することを特徴とする有資格者判定方式。
【請求項2】　請求項1において、有資格者の判定を要求する通信回線は電話回線で、乱数の通知は音声メッセージであることを特徴とする有資格者判定方式。
【請求項3】　請求項1において、有資格者判定装置はホストコンピュータであり、ワンタイムパスワード再生装置はクライアントコンピュータであり、このクライアントコンピュータを前記ホストコンピュータに接続するデータ回線を介してクライアント側からクライアント側で生成した前記ワンタイムパスワードを送って前記ホストコンピュータとの間のデータ転送の資格を得ることを特徴とする有資格者判定方式。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、クライアントから入力されるパスワードにより有資格者を判定する有資格者判定方式に関し、特に、秘密性の保持が確実にできる有資格者判定方式に関する。
【0002】
【従来の技術】従来、この種の有資格者判定方式では、クライアントがホストコンピュータに有資格者の判定を要求する際、ホストコンピュータ内にパスワードを変換する符号化機能を設け、周期的にクライアントのパスワードを変更してパスワードの漏洩に対処している。しかし、この場合の変更周期の問題または変更の煩わしさを避けるのため、パスワードを符号化規則にしたがって変換し、同時にこの変換に同期する機能、文字表示機能、およびホストコンピュータと同一の符号化機能を持たせたＩＣカードをクライアントに事前に配布し、このＩＣカードを利用することにより、有資格者判定の便宜を図っている。
【0003】この方法ではクライアントにＩＣカードを必要とするという問題点がある。
【0004】一方、別に音声入力に応じて有資格者を判定するという技術が、例えば、特開昭62-145295号公報に記載されている。
【0005】この方式では、図4に主要部分の構成概要が示されるように、電話機１１１から公衆通信網３０を介し接続される有資格者判定装置１４０は、網制御回路１４１、スイッチ１４２、音声合成回路１４３、音声認識回路１４４、乱数発生回路１４５、暗証番号メモリ１４６および暗証番号テーブル１４７を備えている。
【0006】ここで、図4に図5のフローチャートを併せ参照して動作機能を説明する。
【0007】電話機１１が公衆通信網３０を介して有資格者判定装置１４０を接続した場合に、有資格者判定装置１４０は音声合成回路１４３から合成音声により質問または要求し、電話機１１１から応答された音声を音声認識回路１４４により認識し内容を確認している。
【0008】まず、有資格者判定装置１４０は、合成音声により電話機１１１の使用者に会員番号を尋ね、音声による会員番号を受け付ける（手順Ｓ１０１）。次に、有資格者判定装置１４０は、受けた音声を会員番号に認識し、この認識した番号を合成音声で通知し電話機１１１から「はい」との確認（手順Ｓ１０２）を得る。
【0009】次いで、有資格者判定装置１４０は、暗証番号の１桁目に対して乱数発生回路１４５から乱数と四則演算子とを発生させて記憶し、電話機１１１の使用者に暗証番号の１桁目に対してこれら乱数および四則演算子による計算を要求（手順Ｓ１０３）する。例えば「暗証番号の１桁目に“４”を加えてください」が要求される。
【0010】計算結果を受けた有資格者判定装置１４０は、受けた計算結果をこれら乱数および四則演算子により逆算し、逆算結果を暗証番号メモリ１４６の１桁目に格納（手順Ｓ１０４）する。ここでは、全桁分が終了していない（手順Ｓ１０５のＮＯ）ので、有資格者判定装置１４０は、暗証番号の次の桁に対して乱数発生回路１４５から乱数と四則演算子とを発生させて記憶し、電話機１１１の使用者に暗証番号の次の桁に対してこれら乱数および四則演算子による計算を要求（手順Ｓ１０６）して、計算結果を受ける手順Ｓ１０４に戻り、手順を繰り返す。
【0011】上記手順Ｓ１０５が“ＹＥＳ”で全桁分の暗証番号の格納が終了した際には、有資格者判定装置１４０は、暗証番号メモリ１４６から逆算結果の暗証番号を読み取って合成音声により電話機１１１の使用者に通知し、電話機１１１から「はい」との確認（手順Ｓ１１１）を得る。
【0012】次いで、有資格者判定装置１４０は、会員番号に対応して登録された暗証番号を格納する暗証番号テーブル１４７から暗証番号を読み取り（手順Ｓ１１

2）、逆算結果の暗証番号と照合して一致を確認（手順S113）して有資格者を判定（手順S114）している。

【0013】

【発明が解決しようとする課題】上述した従来の有資格者判定方式のうち、ICカードを使用する場合ではカード使用の繁雑さ、またはカードの盗難などという問題点がある。

【0014】また、上記公開公報に記載された方式では、音声により電話回線を使用して手順S113において暗証番号が転送されるので、第三者に簡単に盗聴されるという面で問題点がある。また、規模が大きい音声認識装置が使用されているので大規模となり、利用者が音声案内にしたがって暗証番号に対する計算を行うので計算ミスを発生する機会が多く、四則演算では暗証番号に数字のみを使用する必要があるという問題点がある。

【0015】本発明の課題は、これらの問題点を解決して、簡単な操作で、更に秘密性の保持が確実にできる有資格者判定方式を提供することである。

【0016】

【課題を解決するための手段】本発明による有資格者判定方式は、クライアントから入力されるパスワードにより有資格者を判定する有資格者判定方式において、有資格者の判定を行う有資格者判定装置側では、一つの通信回線を介して有資格者の判定要求を受けた際に乱数を発生して前記クライアントに通知すると共にこのクライアントに対して予め定められたパスワードに前記乱数を加味し所定の暗号化式により一回限りのワンタイムパスワードを生成するワンタイムパスワード生成装置と、クライアント側では、有資格者の判定要求をした際に受けた乱数を自己のパスワードに加味し前記暗号化式により一回限りのワンタイムパスワードを生成し前記通信回線とは別の通信回線を介して前記有資格者判定装置へ送るワンタイムパスワード再生装置とを備え、前記有資格者判定装置が、前記ワンタイムパスワード生成装置で生成したワンタイムパスワードと前記ワンタイムパスワード再生装置で生成したワンタイムパスワードとの一致を確認して有資格者と判定している。

【0017】上記構成では、今回限りの乱数およびワンタイムパスワードが生成され、かつ両者はそれぞれ別の通信回線を利用して転送されている。

【0018】また、有資格者の判定を要求する通信回線は電話回線であって、乱数の通知は音声メッセージとすることができる。

【0019】また、有資格者判定装置はホストコンピュータであり、ワンタイムパスワード再生装置はクライアントコンピュータであり、このクライアントコンピュータを前記ホストコンピュータに接続するデータ回線を介してクライアント側から前記ワンタイムパスワードを送って前記ホストコンピュータとのデータ転送の資格を得る構成でもよい。

【0020】また、ワンタイムパスワードは、クライアントのパスワードと発生した乱数とを排他的論理和演算した後、前記暗号化式として所定の生成多項式を用いて生成することもできる。したがって、クライアントのパスワードは数値に限定されることはない。

【0021】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0022】図1は本発明の実施の一形態を示す機能ブロック図である。図1では、本発明に関する部分の構成のみ、およびデータの流れを主に示し、各装置内の制御部および制御線については省略してある。

【0023】図1に示された有資格者判定方式では、クライアント端末10およびクライアントコンピュータ20を有するクライアントが公衆通信網30を介してホストコンピュータ50を利用する際に利用有資格者の判定を行う構成が示されており、ホストコンピュータ50側にワンタイムパスワード生成装置40を設け、クライアントコンピュータ20の内部にワンタイムパスワードの再生装置を備えているものとする。

【0024】クライアント端末10は電話機11およびキーボード12を有するものとし、クライアントコンピュータ20は、ワンタイムパスワード再生装置としてデータ入力部21、パスワードデータ22、EX-OR（排他的論理和回路）部23、データ符号化部24、およびデータ回線接続制御部25を備えるものとする。

【0025】ワンタイムパスワード生成装置40は、ホストコンピュータ50の一部として設けられ、電話回線接続制御部41、着信受付部42、乱数発生部43、音声案内装置44、EX-OR部45、およびデータ符号化部46を備えているものとする。

【0026】また、ホストコンピュータ50は、パスワードテーブル51、ワンタイムパスワードテーブル52、データ回線接続制御部53、パスワード受付部54、およびデータ照合部55を備えるものとする。

【0027】電話機11は公衆通信網30の電話回線に接続している。キーボード12は自己のクライアントコンピュータ20と接続してデータを入力するものとする。電話機11から発呼される呼接続要求には、自己の予め付与されたクライアントID（識別）情報が含まれるものとする。

【0028】データ入力部21はキーボード12とインタフェースしてデータを受け付けるものとする。パスワードデータ22はクライアント自身のクライアントID情報およびパスワードを格納しているものとする。EX-OR部23は、データ入力部21で受けたデータとパスワードデータ22に格納されているパスワードとを入力して排他的論理和演算した結果をパスワードデータ22に格納されているクライアントID情報と共にデータ

符号化部２４へ出力し、データ符号化部２４では入力したデータを暗号化式として下記数式１の生成多項式により演算してワンタイムパスワードを再生するものとする。

$$P(x)=X^{16}+X^{12}+X^{5}+1 \qquad (1)$$

データ回線接続制御部２５は所定のアドレスにより公衆通信網のデータ回線を介してホストコンピュータ５０と接続できる。

【００３０】公衆通信網３０は単一とは限らずどのような構成であってもよい。

【００３１】電話回線接続制御部４１は所定の有資格者判定要求に対するアドレスにより公衆通信網に接続されているものとする。着信受付部４２は、着信を受け付けた際に所定の判定要求に含まれるクライアントＩＤ情報を検出し、クライアントＩＤ情報をもって乱数発生部４３を駆動するものとする。

【００３２】乱数発生部４３は、着信受付部４２から駆動を受け、乱数を発生して音声案内装置４４およびＥＸ－ＯＲ部４５それぞれに通知するものとする。音声案内装置４４は、乱数発生部４３から受けた乱数を音声により電話回線接続制御部４１および公衆通信網３０の電話回線を介して発呼電話機１１に送るものとする。ＥＸ－ＯＲ部４５およびデータ符号化部４６それぞれは、クライアントコンピュータ２０のＥＸ－ＯＲ部２３およびデータ符号化部２４それぞれと全く同一の機能を有するものとする。したがって、ＥＸ－ＯＲ部２３は、クライアントＩＤ情報と乱数発生部４３から発生した乱数とを受けることになる。

【００３３】パスワードテーブル５１は、全てのクライアントそれぞれに対し予め登録されたパスワードを有するものとし、このパスワードはＥＸ－ＯＲ部４５によりクライアントＩＤ情報に対して読み取られるものとする。図１では、従来の設備機能のみしか有しないクライアントにも対応できるようにするため、パスワードテーブル５１がホストコンピュータ５０に備えられているが、全てのクライアントに同一の上記機能設備を備える場合にはワンタイムパスワード生成装置４０に備えることができる。

【００３４】ワンタイムパスワードテーブル５２は、全てのクライアントそれぞれに対しデータ符号化部４６で符号化されたデータをワンタイムパスワードとして記録するものとする。この記録はデータ照合部５５により取り出されるが、記録されたデータの取出しは一回限りで、次回に取り出される記録は新しく符号化されたワンタイムパスワードにより更新されたものである。

【００３５】データ回線接続制御部５３はホストコンピュータ５０のアドレスにより公衆通信網３０のデータ回線を介してクライアントコンピュータ２０のデータ回線接続制御部２５と接続する。パスワード受付部５４は、クライアントコンピュータ２０のデータ符号化部２４で符号化されたワンタイムパスワードおよび発信元のクライアントＩＤ情報をデータ回線接続制御部２５、５３の制御により受け付け、データ照合部５５を駆動するものとする。

【００３６】データ照合部５５はパスワード受付部５４の駆動を受け、受けたクライアントＩＤ情報に対するワンタイムパスワードをワンタイムパスワードテーブル５２から取り出し、別にパスワード受付部５４から受けたワンタイムパスワードと照合し、一致を確認して有資格者を判定するものとする。

【００３７】次に、図１に図２を併せ参照して、ホストコンピュータ側におけるワンタイムパスワード生成装置４０およびホストコンピュータ５０の動作手順の一形態について説明する。

【００３８】ワンタイムパスワード生成装置４０では、最初に、電話回線接続制御部４１が電話機１１から所定のアドレスおよび自己のクライアントＩＤ情報を含む有資格者判定要求を公衆通信網３０の電話回線を介して受け（手順Ｓ１）、着信受付部４２を駆動する。着信受付部４２はクライアントＩＤ情報を検出（手順Ｓ２）しクライアントＩＤ情報をもって乱数発生部４３を駆動する。

【００３９】乱数発生部４３は、駆動を受けて乱数を発生し、一方で音声案内装置４４を駆動して音声案内装置４４により発生した乱数を発呼元の電話機１１へ音声案内メッセージにより送出（手順Ｓ３）する。他方、乱数発生部４３は、駆動の際に受けたクライアントＩＤ情報および発生した乱数をＥＸ－ＯＲ部４５へ送る。

【００４０】ＥＸ－ＯＲ部４５は、受けたクライアントＩＤ情報に対するパスワードをパスワードテーブル５１にアクセス（手順Ｓ４）して読み取り（手順Ｓ５）、このパスワードと乱数とを排他的論理和演算（手順Ｓ６）してデータ符号化部４６にクライアントＩＤ情報と共に送る。

【００４１】データ符号化部４６は受けた演算結果データを上記数式１を用いて符号化（手順Ｓ７）してワンタイムパスワードテーブル５２にアクセス（手順８）する。次いで、データ符号化部４６はワンタイムパスワードテーブル５２における受けたクライアントＩＤ情報に対応するワンタイムパスワードを新しく符号化したデータにより更新（手順Ｓ９）することにより新しいワンタイムパスワードを格納する。

【００４２】一方、データ回線接続制御部５３は、公衆通信網３０のデータ回線を介してクライアントからの接続要求を待つ（手順Ｓ１０のＮＯ）。接続要求には、クライアントＩＤ情報とワンタイムパスワードとが含まれている。手順Ｓ１０が“ＹＥＳ”となり接続要求を受け

た際、データ回線接続制御部５３は接続要求の情報をパスワード受付部５４へ送る。パスワード受付部５４は、接続要求からクライアントＩＤ情報とワンタイムパスワードとを検出（手順Ｓ１１）してデータ照合部５５へ送る。

【００４３】データ照合部５５は、クライアントＩＤ情報に対応するワンタイムパスワードをワンタイムパスワードテーブル５２から読み取り（手順Ｓ１２）、この読み取ったワンタイムパスワードとデータ回線およびパスワード受付部５４を介して受けた接続要求に含まれるワンタイムパスワードとを照合（手順Ｓ１３）する。

【００４４】データ照合部５５は、照合一致（手順Ｓ１４のＹＥＳ）を確認し、接続要求してきたクライアントを有資格者と判定（手順Ｓ１５）する。この有資格者との判定によりホストコンピュータ５０とクライアントコンピュータ２０との間におけるデータ通信が可能になる。上記手順Ｓ１５が“ＮＯ”で不一致の場合には接続要求してきたクライアントを無資格者と判定（手順Ｓ１６）して、ホストコンピュータ５０からクライアントコンピュータ２０に通知すると共にこの接続は切断される。

【００４５】次に、図１に図３を併せ参照してクライアント側におけるクライアント端末１０および上記ワンタイムパスワードを再生するクライアントコンピュータ２０の動作手順の一形態について説明する。

【００４６】まず、ホストコンピュータ５０とのデータ通信を希望するクライアントは、ホストコンピュータ５０に対応する所定のアドレスおよび自己のクライアントＩＤ情報を含む所定の有資格者判定要求を電話機１１から呼接続要求により送出（手順Ｓ２１）する。この呼接続要求により電話機１１は公衆通信網３０を介してワンタイムパスワード生成装置４０を呼び出す。

【００４７】この呼接続要求に対する応答として、上述した手順Ｓ３の音声案内による乱数のメッセージがワンタイムパスワード生成装置４０から送られる。クライアントは、電話機１１により音声案内された乱数値を受け取る（手順Ｓ２２）ので、この乱数値とクライアントＩＤ情報とを含むホストコンピュータ５０への接続要求をクライアントコンピュータ２０と接続するキーボード１２からデータ入力部２１へ入力（手順Ｓ２３）する。

【００４８】データ入力部２１は受けた乱数値とクライアントＩＤ情報とをＥＸ－ＯＲ部２３へ送る。ＥＸ－ＯＲ部２３は、クライアントＩＤ情報によりクライアントに対応するパスワードをパスワードデータ２２から読み取り（手順Ｓ２４）、このパスワードと乱数値とを排他的論理和演算（手順Ｓ２５）してデータ符号化部２４にクライアントＩＤ情報と共に送る。

【００４９】データ符号化部２４は、受けた演算結果データを上記数式１を用いて符号化しワンタイムパスワードを再生（手順Ｓ２６）してクライアントＩＤ情報と共にデータ回線接続制御部２５へ送る。データ回線接続制御部２５は、ホストコンピュータ５０を宛先とし、受けたワンタイムパスワードおよびクライアントＩＤ情報を含む接続要求（手順Ｓ２７）を行う。

【００５０】この接続要求は、公衆通信網３０のデータ回線を介してホストコンピュータ５０を呼び出し、上述の手順Ｓ１５により有資格者判定の応答（手順Ｓ２８のＹＥＳ）を受け、クライアントはホストコンピュータ５０に対してデータ通信が可能（手順Ｓ２９）になる。一方、上記手順Ｓ２８が“ＮＯ”で不適格者判定を受けた場合には、この呼接続は切断（手順Ｓ３０）される。

【００５１】上記説明では一つのクライアントのみであるが、たのクライアントからも上述と同様な手順で動作が実行されるが、すでに接続されている利用者の認証は完了しているためこの利用者に対するワンタイムパスワードがなんらかの理由で無効になっても、ホストコンピュータのサービスに影響を与えることはない。

【００５２】上述したように、クライアントが有資格者判定を要求する際、ホストコンピュータ側から電話回線で受ける音声による応答情報は毎回異なる乱数値であり、また、データ回線でホストコンピュータ側へ送るデータは毎回異なるワンタイムパスワードである。したがって、これら情報またはデータが盗まれても、また、コンピュータ内部のパスワードまたはデータ符号化のための演算式を盗まれても、有資格者判定のパスワードに利用することはできない。

【００５３】上記説明では、クライアント端末からワンタイムパスワード生成装置を呼び出す回線を電話回線としたが、コンピュータ端末から通信制御装置を介してデータ回線により接続し、音声案内に代わり文字メッセージにより応答される構成であってもよい。

【００５４】また、クライアント側でワンタイムパスワードを再生する装置をクライアントコンピュータに備えるとして図示し説明したが、この部分を独立したワンタイムパスワード再生装置としてもよい。

【００５５】このように、上記説明では、機能ブロックおよび動作手順を図示して説明したが、機能の分離併合によるブロック構成の変更、または手順の平行動作または前後の入れ替えなどの変更は上記機能を満たす限り自由であり、上記説明が本発明を限定するものではない。

【００５６】

【発明の効果】以上説明したように本発明による有資格者判定方式によれば、クライアントから入力されるパスワードにより有資格者を判定する有資格者判定方式において、判定要求の際に有資格者判定装置側で発生する乱数をクライアント側に通知し、クライアント側と有資格者の判定を行う有資格者判定装置側との両方それぞれの側で同一の乱数および同一の暗号化式を用いてクライアントのパスワードを暗号化してワンタイムパスワードを生成したのち、乱数を通知した通信回線とは別の通信回

線を用いて有資格者判定装置側に生成されたワンタイムパスワードを集めて照合一致を確認し、有資格者を判定している。

【0057】したがって、今回限りの乱数およびワンタイムパスワードが生成され、かつ両者はそれぞれ別の通信回線を利用して転送されているので、同時に同一の有資格者判定に用いるデータ・情報の漏洩は不可能に近く、秘密性の保持が確実であるという効果が得られる。また、クライアントによる乱数という単純な数字の復唱以外、ワンタイムパスワードが自動的に生成および再生されるので、クライアントの簡単な操作が実現し利便性が確保されるという効果も得ることができる。

【0058】また、ワンタイムパスワードは、クライアントのパスワードと発生した乱数とを排他的論理和演算した後、前記暗号化式として所定の生成多項式を用いて生成しているので、クライアントのパスワードは数値に限定されることなく、文字を使用することもできる。

【0059】また、音声認識回路を用いる場合と比較して小規模構成で実現できる効果がある。

【図面の簡単な説明】

【図1】本発明の実施の一形態を示す機能ブロック図である。

【図2】図1におけるホストコンピュータ側の主要動作手順の一形態を示すフローチャートである。

【図3】図1におけるクライアント側の主要動作手順の一形態を示すフローチャートである。

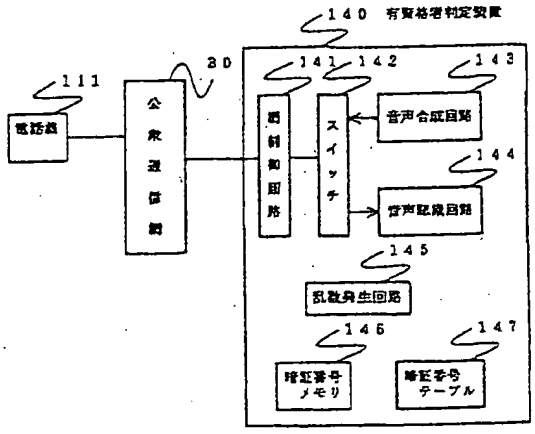
【図4】従来の一例を示す機能ブロック図である。

【図5】図4における主要動作手順の一例を示すフローチャートである。

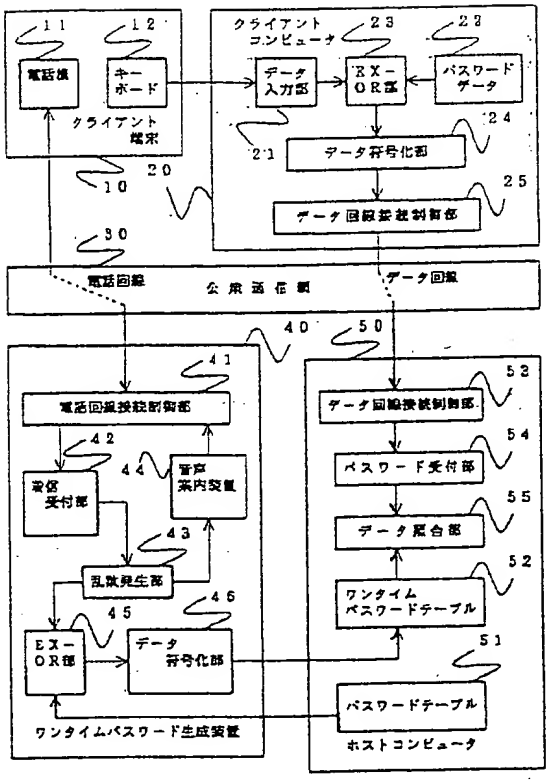
【符号の説明】

10　クライアント端末
11　電話機
12　キーボード
20　クライアントコンピュータ
21　データ入力部
22　パスワードデータ
23、45　EX－OR（排他的論理和回路）部
24、46　データ符号化部
25、53　データ回線接続制御部
40　ワンタイムパスワード生成装置
41　電話回線接続制御部
42　着信受付部
43　乱数発生部
44　音声案内装置
50　ホストコンピュータ
51　パスワードテーブル
52　ワンタイムパスワードテーブル
54　パスワード受付部
55　データ照合部

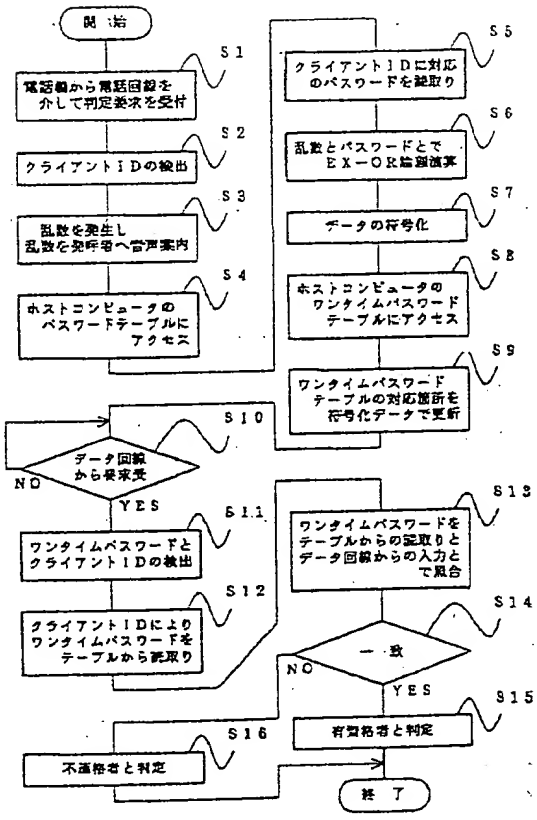
【図4】



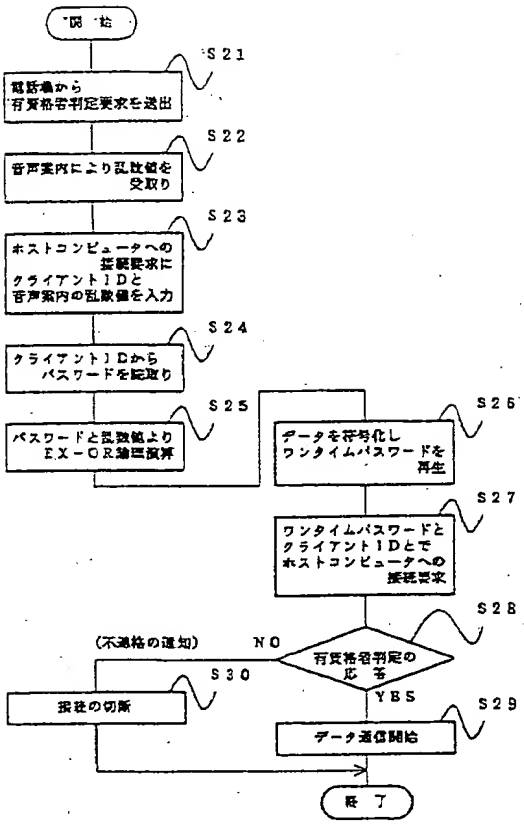
【図1】


11
12
電話機
キーボード
クライアント端末
クライアントコンピュータ
23
22
データ入力部
EX-OR部
パスワードデータ
24
21
データ符号化部
25
データ回線接続制御部
20
10
30
電話回線
公衆通信網
データ回線
40
50
41
電話回線接続制御部
42
着信受付部
44
音声案内装置
43
乱数発生部
46
45
EX-OR部
データ符号化部
ワンタイムパスワード生成装置
52
データ回線接続制御部
54
パスワード受付部
55
データ照合部
52
ワンタイムパスワードテーブル
51
パスワードテーブル
ホストコンピュータ

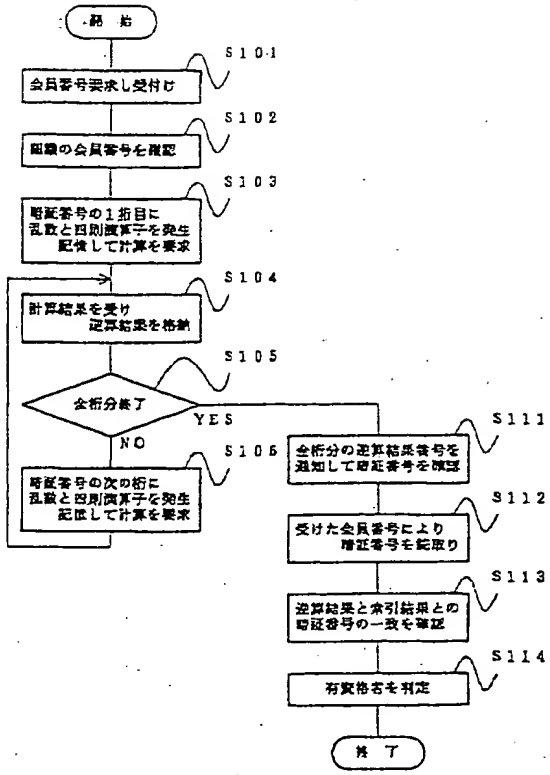
【図2】


開始
S1
電話機から電話回線を介して判定要求を受付
S2
クライアントIDの検出
S3
乱数を発生し乱数を発呼者へ音声案内
S4
ホストコンピュータのパスワードテーブルにアクセス
S5
クライアントIDに対応のパスワードを読取り
S6
乱数とパスワードとでEX-OR論理演算
S7
データの符号化
S8
ホストコンピュータのワンタイムパスワードテーブルにアクセス
S9
ワンタイムパスワードテーブルの対応箇所を符号化データで更新
S10
データ回線から要求受
NO
YES
S11
ワンタイムパスワードとクライアントIDの検出
S12
クライアントIDによりワンタイムパスワードをテーブルから読取り
S13
ワンタイムパスワードをテーブルからの読取りとデータ回線からの入力とで照合
S14
一致
NO
YES
S15
有資格者と判定
S16
不適格者と判定
終了

【図3】


開始
S21
電話機から
有資格者判定要求を送出
S22
音声案内により乱数値を
受取り
S23
ホストコンピュータへの
接続要求に
クライアントIDと
音声案内の乱数値を入力
S24
クライアントIDから
パスワードを記取り
S25
パスワードと乱数値より
EX-OR論理演算
S26
データを符号化し
ワンタイムパスワードを
再生
S27
ワンタイムパスワードと
クライアントIDとで
ホストコンピュータへの
接続要求
S28
有資格者判定の
応答
NO
(不適格の通知)
S30
接続の切断
YES
S29
データ通信開始
終了

【図5】


開始
S101
会員番号要求し受付け
S102
相手の会員番号を確認
S103
暗証番号の1桁目に
乱数と四則演算子を発生
記憶して計算を要求
S104
計算結果を受け
逆算結果を格納
S105
全桁分終了
YES
NO
S106
暗証番号の次の桁に
乱数と四則演算子を発生
記憶して計算を要求
S111
全桁分の逆算結果番号を
通知して暗証番号を確認
S112
受けた会員番号により
暗証番号を記取り
S113
逆算結果と索引結果との
暗証番号の一致を確認
S114
有資格者を判定
終了